IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	CASE NO. 1:15-CR-275
	)	
Plaintiff,	)	JUDGE DAN AARON POLSTER
	)	
v.	)	
	)	**MOTION TO SUPPRESS**
	)	**OR, IN THE ALTERNATIVE,**
JOHN CLEMENTS,	)	**MOTION TO RECONSIDER**
	)	**DEFENDANT'S MOTION**
Defendant.	)	**TO COMPEL DISCOVERY**
	)	

Now comes Defendant, John Clements, by and through undersigned counsel, and hereby respectfully requests that this Honorable Court suppress any and all evidence seized during the undercover investigation that was conducted by the Lake County Sheriff's Department in this case as well as any evidence that was seized pursuant to the search warrant that was executed on June 3, 2014. In the alternative, counsel requests that this Honorable Court reconsider its previous decision denying defense counsel's Motion to Compel information regarding the Shareaza LE software that was used during the undercover investigation of this case.

Defendant so moves pursuant to the Fourth and Fourteenth Amendments to the United States Constitution, Rule 16 of the Federal Rules of Criminal Procedure as well as *Brady v. Maryland*, 373 U.S. 83 (1963) and *Giglio v. United States*, 405 U.S. 150 (1972). Reasons in support of the instant request are set forth more fully in the Memorandum in Support, which is attached hereto and incorporated herein by express reference.

Respectfully submitted,

/s/ Eric C. Nemecek
IAN N. FRIEDMAN (0068630)
ERIC C. NEMECEK (0083195)
Counsel for Defendant
Friedman & Nemecek, L.L.C.
1360 E. 9th Street, Suite 650
Cleveland, OH 44114
Phone: (216) 928-7700
Email: inf@fanlegal.com
ecn@fanlegal.com

CERTIFICATE OF SERVICE

A copy of the foregoing Motion has been served electronically this 16th day of March, 2016, to Brian McDonough, Assistant United States Attorney, United States Courthouse, Northern District of Ohio, 801 Superior Avenue W., Suite 400, Cleveland, Ohio 44113.

/s/ Eric C. Nemecek
IAN N. FRIEDMAN
ERIC C. NEMECEK
Counsel for Defendant

MEMORANDUM IN SUPPORT

I. FACTS AND PROCEDURAL HISTORY

Defendant, John Clements, is charged with one count of receiving and distributing child pornography in violation of 18 U.S.C. § 2252(a)(2)[1] and one count of possessing child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). The Government's initial discovery response referenced a specialized computer software program, Shareaza LE, that was utilized by law enforcement agents during their investigation in this case. According to the discovery materials, Detective Don Seamon utilized Shareaza LE, in conjunction with Grid Cop ("CPS") website, to search for Internet Protocol ("IP") addresses of network users who have recently been identified as having files of child pornography available for download.

In his report, Detective Seamon notes that the CPS database identified a particular IP address as having 395 Child Notable files. The report further states that this IP address has been directly browsed on two (2) occasions between February 25, 2014 and May 5, 2015. Detective Seamon asserts that on May 5, 2014, he was able to successfully complete four (4) single source download files of suspected child pornography and several incomplete files from this IP address.

On May 17, 2014, Detective Seamon utilized the American Registry for Internet Numbers ("ARIN") and determined that the aforementioned IP address was registered to AT&T Services. That same date, Detective Seamon requested that the Lake County Prosecutor's Office issue a Subpoena to AT&T Services to obtain subscriber information for this IP address. The response to said Subpoena indicated that Clements was the user

[1] Count 1 contains a date range of February 25, 2014 through May 5, 2014.

assigned to that IP address. The information generated from Shareaza LE, CPS and the Subpoena was utilized by Detective Seamon in order to obtain a search warrant for Clements' residence.

On June 2, 2014, Detective Seamon prepared an Affidavit in support of his request for a search warrant of Clements' residence. A copy of Detective Seamon's Affidavit is attached hereto as Exhibit "A" and is incorporated herein by express reference. The Affidavit was submitted to and approved by a Judge of the Lake County Court of Common Pleas that same day. On June 3, 2014, law enforcement officers executed the search warrant at Clements' home and seized several items, which were subsequently forensically analyzed by law enforcement agents.

As a result of the Government's investigation in this case, Clements was indicted on July 21, 2015 with the foregoing offenses. After receiving the Government's initial discovery response, defense counsel retained the services of Tami Loehrs of Loehrs & Associates, L.L.C., to conduct an independent forensic examination of the electronic evidence that was seized in connection with the search warrants. Ms. Loehrs has extensive experience conducting forensic examinations in child pornography cases and is acutely familiar with the investigative aspects of such cases, including the Government's use of specialized forensic software.

Based upon her review of the evidence as well as her prior experience with law enforcement's use of modified software programs, Ms. Loehrs opines that an independent forensic examination of the Shareaza LE software is necessary in order to determine the validity and/or reliability of the Government's forensic evidence – which was a product of

the Shareaza LE software – as well as to determine whether the software conducted a search of Clements' computer beyond the scope of what was publicly available.

Ms. Loehrs authored an Affidavit containing a detailed explanation of how the use of the Shareaza LE software could conceivably have conducted a search of Clements' computer – prior to the issuance of any search warrant(s) – for files that were not otherwise publicly available. A copy of Ms. Loehrs' Affidavit is attached hereto as Exhibit "B" and is incorporated herein by express reference. Specifically, Ms. Loehrs notes that "[i]n this case, there is particular concern regarding the ability of the [law enforcement] software going beyond the scope of "publicly available information." In support of this contention, Ms. Loehrs explains that the discovery materials contain a Screen Shot of Clements' computer, which revealed information regarding the user's (*i.e.* Clements') potential key word searches and "key strokes." *See* Exhibit "B." Importantly, "[t]his type of data is not publicly available information, is not known by the user, and cannot be obtained with any commercially available P2P[2] file sharing software." *See* Exhibit "B."

Ms. Loehrs also discusses her knowledge of and prior experience with law enforcement's use of this type of software during their investigations in similar cases. She contends that the CPO software herein at issue was developed by William Wiltse, who was formerly employed by a Florida-based company, TLO. Ms. Loehrs explains that Wiltse develops software that is utilized by law enforcement agencies in their investigations of child exploitation crimes. Ms. Loehrs also indicates that she has been involved in

[2] "P2P" is an acronym for Peer-to-Peer, which describes a specific software program that allows users connected to the same network to locate and download desired content.

numerous cases throughout the country wherein this software – or variations of the software – was at issue. *See* Exhibit "B."

Although Wiltse was formerly employed by TLO, the undersigned has learned that this Company filed for Bankruptcy in 2013 and, at the present time, no longer appears to be operational. However, counsel has determined that Wiltse is currently employed with the Child Rescue Coalition, Inc. (hereinafter "CRC"), which is located at the same physical address/location as TLO. Furthermore, a review of the CRC's website indicates that many – if not all – of the same individuals who were responsible for developing and implementing the CPO software are also employed at the CRC.[3] Regardless of which particular Company developed the Shareaza LE software, the undersigned submits that the materials herein requested are available to the Government insofar as its agents have access to – and continue to utilize – the software during the course of its investigations in these cases.

In response to Ms. Loehrs' conclusions, defense counsel sent a letter to Assistant United States Attorney Brian McDonough on December 8, 2015, requesting that he produce discovery relating to Shareaza LE software program that was utilized by law enforcement in this case. A copy of the December 8th letter is attached hereto as Exhibit "C" and is incorporated herein by express reference. Having received no response from the Government, counsel sent a second letter to AUSA McDonough on December 14, 2015,

[3] A Subpoena *duces tecum* was issued to CRC requesting the same materials and/or access as set forth in the instant request. The process server has informed the undersigned that the Subpoena was properly served on or about January 13, 2016. To date, counsel has not received any response to the Subpoena.

requesting that the same material be provided forthwith. A copy of the December 14th letter is attached hereto as Exhibit "D" and is incorporated herein by express reference.

On or about December 21, 2015, the undersigned spoke with AUSA McDonough over the phone to discuss the nature of the discovery request – *i.e.* an independent forensic analysis of the Shareaza LE software. During that conversation, AUSA McDonough indicated that he would obtain some additional discovery materials from law enforcement regarding the software that had not previously been provided to the undersigned, including the file logs that were generated by the Shareaza LE software during the investigation of this case. He also stated that he would discuss counsel's request for access to the Shareaza LE software with the agents.

The Government provided the file logs to defense counsel on January 8, 2016 along with a letter. Counsel again queried as to whether its expert would be permitted access to the Shareaza LE software as originally requested. On January 13, 2016, AUSA McDonough responded via email and indicated that: "[t]he Government will not be providing the Shareaza LE software to your expert in this case. Among other reasons, the software is sensitive in nature, non-public, and proprietary." A copy of the Government's January 8th letter is attached hereto as Exhibit "E" and is incorporated herein by express reference.

On January 26, 2016, the parties appeared before the Court for a pretrial hearing. At that time, the Court heard arguments from counsel regarding the specific issues set forth in Defendant's Motion to Compel. After considering those arguments, the Court denied counsel's request to compel production of the Shareaza LE software and any information related thereto. However, the Court directed the parties to conduct a teleconference with

the respective efforts in order to determine whether the questions raised in the Motion to Compel and/or testing of the software could be addressed without the need for further litigation.

At the Court's directive, the parties conducted a teleconference with William Wiltse and Tami Loehrs on February 5, 2016. Mr. Wiltse provided information regarding the functionality of the software. Mr. Wiltse also confirmed that he is the only person who has access to the source code for the software and that the software has never been subjected to testing or analysis to verify its accuracy and/or purported limitations. Although he maintains that the software does not provide the Government with any information that it could not obtain through publicly available means, counsel submits that the evidence provided in this case does not support said conclusion.

During that teleconference, counsel inquired as to whether it would be possible to test some – or all – components of the software without compromising ongoing investigations or revealing any sensitive or confidential information, which were issues that the Government raised in its oppositional Brief. Mr. Wiltse indicated his willingness to review the discovery information regarding the specific software that was utilized in this case and advise the parties as to whether any independent testing of the software could be conducted. Mr. Wiltse stated that he would follow up with AUSA McDonough regarding his determinations in the coming weeks.

Upon information and belief, Mr. Wiltse was unable to contact AUSA McDonough until March 1, 2016. At that time, he indicated that the software could not be made available for independent analysis as originally requested. Thereafter, the parties appeared

for a hearing on March 2, 2016, and notified the Court as to the status of this issue. The Court instructed the undersigned to submit any additional information and/or evidence regarding its concerns about the Shareaza LE software and/or its contention that the use of said software in this case violated Clements' Fourth Amendment rights.

As the foregoing information establishes, counsel has made reasonable and repeated efforts to obtain the requested materials and access to the Software through the discovery process since determining that such information was necessary for purposes of defending the charges in this case. At the present time, both the Government and Mr. Wiltse maintain their opposition to any independent analysis of the Shareaza LE software as requested.

Based upon the particular facts and circumstances of this case, counsel respectfully submits that the use of the Shareaza LE software violated Clements' Fourth Amendment rights under the United States Constitution, thereby warranting suppression of any evidence generated through use of that software as well as any evidence seized pursuant to the warrant that was issued in this case. Alternatively, Clements respectfully requests that this Honorable Court reconsider its previous denial of the Motion to Compel and Order the Government and/or Mr. Wiltse to allow for independent testing of the Shareaza LE software.

II. LAW AND ARGUMENT

A. The Shareaza LE software conducted a warrantless search of Clements' computer.

The United States Constitution grants defendants charged with a criminal offense the right to be free from unreasonable searches and seizures. The Fourth Amendment of the United States Constitution provides in pertinent part as follows:

> . . . the right of the people to be secure in their persons, houses, papers and affects against unreasonable searches and seizures, shall not be violated and no warrant shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the person or thing to be seized.

See U.S. Const. Amend. IV. The Fourth Amendment thus protects individuals against unreasonable governmental searches and seizures. A warrantless search is per se unreasonable, unless an exception to the warrant requirement applies. *Katz v. United States*, 389 U.S. 347, 357 (1967). Furthermore, once a defendant demonstrates that he was subjected to a warrantless search or seizure, the burden shifts to the Government to establish that the search or seizure was constitutionally permissible.

1. Relevant undisputed facts.

Before addressing the merits of Clements' argument, it is important to note the relevant facts regarding this issue about which the parties agree. First, it is undisputed that Clements installed and used version 2.7.4 of Shareaza, which is a publicly available Peer to Peer (hereinafter "P2P") Program used to search for and download files from other "peer members" – *i.e.* other users of the P2P network. Likewise, the parties agree that law enforcement agents utilized Shareaza LE during the course of their investigation of this case. There is no dispute that Shareaza LE is a modified version of the publicly available

software, meaning that it has been altered to operate in a different manner than the publicly available version of the software.

The Shareaza LE software was developed by Wiltse in his capacity as a private citizen. The Shareaza LE software, including its tools and components, is copyrighted. Furthermore, the source code for the software has never been distributed to any third parties, including law enforcement agencies. In fact, Wiltse maintains that the source code has never been, and will not be, distributed to any law enforcement agency at the municipal, state or federal level.

As Wiltse explains, it is not possible to authenticate the function of the software or validate its calibration without the source code. In other words, because law enforcement officers do not have access to the source code, they are unable to confirm exactly how the software functions. Furthermore, Wiltse informed the parties that the Shareaza LE software itself has never been independently tested or subjected to peer review, and that no reports or publications exist regarding the functionality or reliability of the software.

In summation, the following facts are not in dispute:

1.) Wiltse created Shareaza LE software;

2.) Wiltse *claims* that the Shareaza LE software only provides information that is publicly available – that is, information that is similarly accessible through use of the publicly available version of the Shareaza software;

3.) Wiltse has not provided the source code for the Shareaza LE software to any third parties, including law enforcement officers;

4.) the Shareaza LE software has never been independently tested to verify that it operates in the manner described by Wiltse; and

5.) without the source code or independent testing of the Shareaza LE software, it is impossible to determine that the Shareaza LE software operates in the limited manner described by Wiltse.

2. The information obtained by the Shareaza LE software was not in "plain view."

As the Court is aware, the Fourth Amendment prohibits the Government from conducting a warrantless search and seizure of evidence subject to a few limited exceptions. One such exception, known as the "plain view" exception, is relevant to the instant issue. In order for the "plain view" exception to apply, three (3) requirements must be satisfied: the officer's intrusion into the location where the evidence is located must be lawful, the discovery of the evidence must be inadvertent, and the incriminating nature of the evidence must be immediately apparent. *Texas v. Brown*, 460 U.S. 730, 739 (1983).

Here, the Government argues that no warrant was required in order to operate the Shareaza LE software because the software simply provided the Government with information that was otherwise publicly available – *i.e.* in plain view. According to the Government, the Shareaza LE software operates in the same limited capacity as the publicly available software. In other words, the same information would be available to anyone who used the publicly available version of the software, including the specific version at issue in this case, to wit: Shareaza version 2.7.4.

As discussed more fully *infra*, the Shareaza LE software does not operate in the limited capacity described by the Government. Rather, the Shareaza LE software allows law enforcement to obtain information that would not otherwise be accessible through the publicly available version of the software in at least two (2) distinct respects. First, the

Shareaza LE software allows the Government to obtain other users' search term history and/or "key strokes." Secondly, the Shareaza LE software allows the Government to access portions of the users' computers that the users have not made accessible to the public. Because this information is not available through the use of the publicly available version of Shareaza, and in light of the fact that no warrant was obtained prior to utilizing the Shareaza LE software in this case, the undersigned respectfully submits that all evidence seized in connection with the Shareaza LE software – both directly and derivatively – must be suppressed.

a. The Shareaza LE software conducted a warrantless search of Clements' search history on the P2P network.

The Government denies that any Fourth Amendment violation occurred in this case. The Government's argument is premised upon its contention that the Shareaza LE software did not provide the Government with any information from Clements' computer that was not otherwise in "plain view" – that is, information that Clements made publicly available. In other words, the Government maintains that this same information would have been accessible to other users of the P2P network utilizing the publicly available version of the Shareaza software.

First, it is important to note that the Government's "plain view" argument is predicated entirely upon the representations made by Wiltse concerning the Shareaza LE software's limitations. As aforementioned, the Government has never been provided with the source code for the Shareaza LE software, nor have they conducted any independent testing of that program. Thus, the Government is unable to definitively establish that the

Shareaza LE software only provides information that is in "plain view" or that other P2P users have made publicly available.

Contrary to the Government's speculative arguments, the evidence in this case confirms that the Shareaza LE software obtained information from Clements' computer that was not in "plain view." Specifically, the Government's discovery response included a report containing information that was generated by the Shareaza LE software during the undercover investigation of Clements. This report includes key word searches that Clements allegedly made while using the publicly available version of the Shareaza software. A copy of this report is attached hereto as Exhibit "F" and is incorporated herein by express reference.

The undersigned respectfully submits that a P2P network user's search term history or "key stroke" information are not matters that are publicly available or otherwise in plain view. In support of this contention, counsel directs the Court's attention to two (2) independent sources of information that establish this fact, to wit: Loehrs' Affidavit and the independent demonstration, both discussed more fully *infra*.

i. Loehrs' Affidavit

As set forth in Ms. Loehrs' Affidavit, the report generated by the Shareaza LE software contains information regarding keyword searches conducted by Clements' IP address. Ms. Loehrs further opines that the Shareaza LE software is capable of capturing "key strokes" for a suspect's computer, which is another means of determining the specific search history for public users of the P2P network. *See* Exhibit "B." Ms. Loehrs notes that this type of information is not publicly available to other users of the P2P network insofar

as it is not knowingly shared by the user and cannot be obtained with any commercially or publicly available version of the Shareaza software. *See* Exhibit "B."

ii. Recorded demonstration

In anticipation of filing the instant Motion, counsel downloaded the specific version of the Shareaza software that was used by Clements in this case, to wit: Shareaza version 2.7.4. After downloading said software, counsel conducted various searches and downloads of media files in order to determine whether other users' search term history or "key strokes" would be accessible. Counsel made a recording of this process, a copy of which is attached hereto as Exhibit "G" and is incorporated herein by express reference. As this recording establishes, the publicly available Shareaza software does not provide information regarding users' search terms or search history.

The recording begins with the user downloading the publicly available version of Shareaza that was found on Clements' computer in this case. The recording then shows the installation of the software with the user selecting the default terms. Thereafter, the recording depicts the user conducting various searches for files using the search engine component of the software. The recording then shows the user selecting other P2P network users and browsing their shared folders – that is, the particular files that the user has made available for download to other P2P users on the network.

Through the browser process, the user is able to obtain certain information regarding the other P2P network user. For instance, the user is able to view the shared files for the other user, including the file names, hash values, file extensions and the IP address for the other user. Importantly, no information regarding the other user's search term

history or "key strokes" is provided. Furthermore, a review of the user settings, which is also captured on the recording, does not contain any options that would allow the user to share information regarding their search history or "key strokes."

Both Ms. Loehrs' Affidavit and the attached recording clearly establish that a P2P user's search terms and keyword search history are not matters that are made publicly available or can otherwise be deemed in "plain view." Despite the Government's contentions, such information is not available to other P2P network users operating the publicly available version of the Shareaza software. Because this information is not in plain view, and in light of the fact that no warrant was obtained prior to utilizing the Shareaza LE software, counsel submits that any information obtained pursuant to the Shareaza LE software – both directly and derivatively – must be suppressed.

b. The Shareaza LE software conducted a search of Clements' computer beyond the shared folder of his computer.

The Government maintains that there is no Fourth Amendment violation in this case insofar as the particular files that law enforcement allegedly downloaded from Clements' computer were contained in his shared folder. To that end, the Government's argument hinges upon a determination that the particular files that were viewed and downloaded by the Shareaza LE software were, in fact, contained within the shared folder of Clements' computer. In other words, no warrant is required if the user (*i.e.* Clements) made the particular files that were viewed and downloaded available to other P2P users (*i.e.* Detective Seamon) on the P2P network.

In the case at bar, Ms. Loehrs' forensic examination confirmed that none of the files identified by Detective Seamon during the undercover investigation of this case were located on Clements' computer. *See* Exhibit "B." Ms. Loehrs' further explained that although there are text fragments of files contained on one of the devices, there is no evidence to substantiate that any of these files were contained in the "shared" folder of the computer at the time that they were allegedly identified and downloaded by the Shareaza LE software. *See* Exhibit "B." Thus, to the extent that any of the foregoing files were, in fact, on Clements' computer at the time of the undercover investigation, there is no evidence indicating that they were stored in the shared folder of his computer – that is, they were not in "plain view" or otherwise publicly available. Assuming, without conceding, that these files did exist on Clements' computer at the time of the undercover investigation, the viewing and retrieval of said files by the Shareaza LE software constitutes a warrantless search in violation of Clements' Fourth Amendment rights.

3. The evidence seized pursuant to the search warrant must be suppressed as "fruit of the poisonous tree."

The Fourth Amendment guarantees the people's right to security in their persons, houses, papers, and effects against unreasonable searches and seizures. U.S. Const. amend. IV. When an illegal search or seizure occurs, the exclusionary rule applies to evidence obtained during the illegal police conduct and its derivative uses. *Silverthorne Lumber Co., Inc. v. United States*, 251 U.S. 385, 392 (1920); *see also Weeks v. United States*, 232 U.S. 383, 393 (1914). The "fruit of the poisonous tree" doctrine suppresses evidence obtained through police misconduct. *Walder v. United States*, 347 U.S. 62, 64-65 (1954).

The "fruits" of a Fourth Amendment violation include tangible items actually seized or observed in an illegal search, words overheard during the course of unlawful activity, or confessions or statements made during an illegal arrest or detention. *United States v. Crews*, 445 U.S. 463, 470 (1980). "[S]tatements given during a period of illegal detention are inadmissible even though voluntarily given if they are the product of the illegal detention and not the result of an independent act of free will." *Royer*, 460 U.S. at 501; *see also Kaupp*, 538 U.S. at 633 (reconfirming suppression of evidence obtained during a period of illegal seizure unless the statement was an act of free will sufficient to purge the primary taint of the unlawful seizure).

In *Wong Sun v. United States*, 371 U.S. 471, 487-88 (1963), the Supreme Court held that the "taint" on such evidence does not arise from the illegal conduct. Instead, a court suppresses such evidence after inquiring "whether, granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint." If evidence results from "exploited illegality," a court must suppress it; evidence "attenuated" from the taint may be allowed. *Id.*

Here, the Shareaza LE software was used to identify Clements' IP address and to allegedly download files of suspected child pornography during the course of the undercover investigation. The purported downloads form the entire basis for the receipt and distribution offense set forth in Count 1 of the Indictment. To that end, the Government's ability to prove the first element of the distribution charges, that Clements "knowingly distributed" child pornography by use of his computer, is dependent upon

whether the downloaded files were "publicly available." Moreover, all evidence relied upon to obtain the search warrant – including the issuance of the Subpoena to AT&T Services as well as the Affidavit in support of the search warrant – was a product of the Shareaza LE software.

As previously noted, the Shareaza LE software obtained information that was not in "plain view" or otherwise made publicly available in violation of Clements' Fourth Amendment rights. Therefore, all evidence that was directly generated by the Shareaza LE software would be subject to suppression. Likewise, any evidence seized as a result of the Shareaza LE software, including all evidence seized pursuant to the search warrant that was issued in this case, must also be suppressed as "fruits of the poisonous tree." In essence, because the search and seizure of Clements' devices were predicated upon a warrantless search of his computer, suppression of any evidence generated by the Shareaza LE software – both directly and derivatively – is warranted.

B. The use of the Shareaza LE software violated the Federal Wiretap Act

The federal Wiretap Act is codified at 18 U.S.C. § 2510, *et seq*. In order to establish a violation of the Act, it must be shown that the defendant "(1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device." *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 18 (1st Cir. 2004). As set forth below, it is clear that the use of the Shareaza LE software violated the federal Wiretap Act in this case.

1. Acquisition of "content."

The Wiretap Act defines "contents" as "any information concerning the substance, purport, or meaning of th[e] communication [at issue]. *See* 18 U.S.C. § 2510(8). However, not all forms of content are protected by the Act. The United States Supreme Court has drawn an important distinction between the warrantless seizure of "extrinsic information" and the underlying content of the communication itself. *See Smith v. Maryland*, 442. U.S. 735 (1979). In *Smith*, the Supreme Court found no Fourth Amendment violation from the Government's warrantless use of a pen register, explaining that, unlike the warrantless wiretapping at issue in *Katz v. United States*, 389 U.S. 347 (1967), pen registers do not acquire the contents of communications. *Smith*, 442 U.S. at 741.

Unlike the seizure of "extrinsic information" such as that produced by a pen register, the federal Wiretap Act governs the interception of communication contents. *See* 18 U.S.C. 2510(4); *see also* 18 U.S.C. § 2511(1)(a). While the line between "extrinsic content" and protected communications is dependent upon the particular facts and circumstances of a given case. As a leading treatise on criminal procedure explains:

> the line between content and non-content information is inherently relative. If A sends a letter to B, asking him to deliver a package to C at a particular address, the contents of that letter are contents from A to B, but mere non-content addressing information with respect to the delivery of the package to C. In the case of e-mail, for example, a list of e-mail addresses sent as an attachment to an e-mail communication from one person to another are contents rather than addressing information.

See Wayne R. LaFave, et al., 2 Crim. Proc. § 4.4(d) (3d ed.).

A recently de-classified opinion from the Foreign Intelligence Surveillance ("FISA") Court provides pertinent guidance on this issue. In analyzing whether there was statutory authority for the National Security Agency surveillance program in the context of Universal Resource Locators,[4] the FISA Court observed that the Government possessed trap and trace authority over "dialing, routing, addressing, and signaling information…provided, however, that such information shall not include the contents of any information." *See* [Redacted], No. PR/TT [Redacted] (FISA Ct. 2010), available at *http://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf*. at 26, *quoting* 18 U.S.C. § 3127(4). To further clarify the distinction between "extrinsic" and protected communications, the FISA Court provided an additional explanation that is relevant to the instant matter: "if a user runs a search using an [i]nternet search engine, the 'search phrase would appear in the URL after the first forward slash' as part of the addressing information, but would also reveal contents, *i.e.*, the "substance" and "meaning" of the communication…that the user is conducting a search for information on a particular topic." *Id*. at 32, *quoting* In re Application of the U.S., 396 F. Supp.2d 45, 49 (D. Mass. 2005).

Similarly, the Ninth Circuit Court of Appeals has previously held that queried URL's are content if, but only if, they produce words from a search engine query. *See In re Zynga Privacy Litigation*, 750 F.3d 1098, 1108-09 (9th Cir. 2014). The Ninth Circuit explained that "[a] user's request to a search engine for specific information could constitute a

[4] Universal Resource Locators ("URL") are location identifiers that provide a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. In essence, a URL is a means to access an indicated resource, such as a web page.

communication such that divulging a URL containing that search term to a third party could amount to disclosure of the contents of a communication. *Id.*; *see also United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008)(noting that warrantless capture of URL's is more constitutionally problematic than the warrantless capture of an IP address because a URL identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity.

The House Judiciary Committee has taken an analogous position in its PATRIOT Act report. Specifically, the Committee stated that a pen register order "could not be used to collect information other than 'dialing, routing, addressing, and signaling' information, such as the portion of a URL specifying Web search terms or the name of the requested file or article." *See* H. Rep. No. 107-36, at 53.

Considering the parallels between URL's and the particular facts and circumstances of this case, it is indisputable that Clements' search term history constitutes protected communications under the federal Wiretap Act. In other words, Clements is able to establish that the Government obtained or acquired "content" without a warrant contrary to the provisions of the federal Wiretap Act.

2. There are no applicable exceptions to the Wiretap Act in this case.

Even if a party improperly acquires "content" in contravention of the Act, a court may nevertheless affirm the conduct if the provisions of 18 U.S.C. § 2511(2)(d) are satisfied. Specifically 18 U.S.C. § 2511(2)(d) sets forth that:

> [i]t shall not be unlawful…for a person not acting under the color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication…unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

See 18 U.S.C. § 2511(2)(d). Stated differently, a party who is the intended recipient of any electronic transmission that they acquired and tracked cannot be said to have violated the federal Wiretap Act insofar as they were a "party" to the communication. Importantly, the burden is on the Government to establish that this exception applies. *See 7 Fifths Old Grand-Dad Whiskey v. United States*, 158 F.2d 34, 36 (10th Cir. 1946)(holding that "when a criminal statute sets forth an exception , which exception is not part of the crime, but operates to prevent an act otherwise included in the statute from being a crime, the burden is on the defendant to bring himself within the exception).

In order to determine whether law enforcement officers were "parties" to Clements' electronic transmissions at issue, it is necessary to first define the specific transmissions at issue. In the case at bar, Clements' is alleged to have utilized the Shareaza software to search for and download child pornography. While law enforcement subsequently conducted downloads from Clements' computer, it is Clements' searches that are the subject "electronic communications" for purposes of the instant analysis. Specifically, the

Shareaza LE software permitted law enforcement to obtain information (*i.e.* search terms) that Clements had communicated to the Shareaza network.[5] Although these search terms arguably were "communicated" to other P2P users who made the particular file of interest available for download, law enforcement officers were not a party to these electronic transmissions.

As discussed *supra*, Clements' search terms would not be disclosed to other users on the P2P network, even users from whom he was downloading files. Thus, law enforcement needed an associative device (*i.e.* Shareaza LE) that was capable of capturing communications sent by Clements and intended for Shareaza network or other specific users on the Shareaza network. Because Clements did not communicate directly with law enforcement officers regarding the particular files that he was searching for and/or downloading from other P2P network users, law enforcement was forced to acquire that information from transmissions to which they were not a party – here, through use of the Shareaza LE software.

In summation, law enforcement officers were not the intended recipients of the transmissions herein at issue – *i.e.* the search terms utilized by Clements to search for and download particular files. Accordingly, the Government's conduct is not justified under 18 U.S.C. § 2511(2)(d). Based upon the foregoing analysis, counsel respectfully submits that law enforcement's use of the Shareaza LE software in this case violated the federal Wiretap Act.

[5] The Shareaza LE software provided law enforcement with information regarding search terms that Clements' had utilized on the P2P network – that is, searches that Clements

3. Suppression of the evidence is warranted.

The consequences for a violation of the federal Wiretap Act are set forth in 18 U.S.C. § 2515. That statute provides that:

> [w]henever any wire or oral communication has been intercepted, *no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial*, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

See 18 U.S.C. § 2515. (Emphasis added).

The undersigned acknowledges that the above-cited language does not *per se* mandate the suppression of electronic communications seized in violation of the federal Wiretap Act. *See United States v. Meriwether*, 917 F.2d 955, 960 (6th Cir. 1990)("[Title III] does not provide an independent statutory remedy of suppression for interceptions of electronic communications"). However, Clements respectfully submits that suppression of the unlawfully obtained evidence is appropriate in this case.

First, it is important to note that the similarities between the definition of wire communications and electronic communications in 18 U.S.C. § 2510 indicate that distinguishing the two types of communication is redundant. The almost identical and overlapping nature of wire and electronic communications make it very difficult for even the sophisticated reader to clearly delineate any line of demarcation. Both forms of communications involve the transference of information by wire. Thus, it is reasonable to

---

conducted apart from law enforcement's investigation of this case.

infer that certain types of electronic communications are, by their very nature, "wire communications" insofar as they are transmitted by wire.

As society's reliance upon and use of technology continues to grow, it is objectively reasonable for citizens to expect that their electronic communications will be provided the same degree of protection given to wire or oral communications, irrespective of the statutory language. Regardless of whether a private communication travels through air or cyberspace, the medium of communication should not have an impact on the protection of privacy given by the law. Just as the transition of the law developed during the telephone era and other forms of wire devices, the law should conform to the changing needs of the society.

Secondly, although the technical language of the Wiretap Act may not provide for the suppression of unlawfully intercepted electronic communications, it is important to not lose sight of the principles and purposes underlying the Wiretap Act — protecting a citizen's "reasonable expectation of privacy." *Katz v. United States*, 389 U.S. 347, 353 (1967). Even though the Wiretap Act is an extension of Fourth Amendment protections, it does not supersede or nullify the protections afforded under the United States Constitution. As a prominent legal scholar has noted, "the Supreme Court has interpreted the United States Constitution as providing a fundamental 'right to privacy', located within the undefined 'penumbras' of the Bill of Rights." Katherine A. Oyama, *E-Mail Privacy After United States v. Councilman: Legislative Options For Amending ECPA*, 1 Berkeley Tech L.J. 499 (2006), *citing* In *Griswold v. Connecticut*, 381 U.S. 479, 483-85 (1965)(holding that the United States Constitution protects the right to privacy although its text does not explicitly reference the

term "privacy"). Accordingly, this Court must still consider and apply the principles underlying the Fourth Amendment to the United States Constitution in determining whether the Government's use of the Shareaza LE software violated Clements' legitimate privacy rights and interests.

Here, it is clear that Clements had a legitimate expectation of privacy in the electronic communications that were made through the P2P network. Furthermore, in light of the advancements in technology and the prevalence of its use, Clements' expectation of privacy is one which society should recognize as reasonable. Therefore, the Government's surreptitious and warrantless interception of his electronic communications not only violated the express provisions of the federal Wiretap Act, but also Clements' Fourth Amendment rights. As such, Clements submits that this Honorable Court must suppress any evidence seized – both directly and derivatively – through the Shareaza LE software.

C. The use of Shareaza LE violated the Stored Communications Act.

The Stored Communications Act ("SCA") is a product of congressional recognition that neither existing federal statutes nor the Fourth Amendment protected against potential intrusions on individual privacy arising from illicit access to "stored communications in remote computing operations and large data banks that stored e-mails." *Garcia v. City of Laredo, Tex.*, 702 F.3d 788, 791 (5th Cir. 2012). To establish a violation of the SCA, a party must show that the defendant "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in

such system." *See* 18 U.S.C. § 2701(a).

The SCA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *See* 18 U.S.C. § 2510(15). Courts have interpreted the SCA to apply to providers of a communication service such as telephone companies, Internet or e-mail service providers, and bulletin board services. *Garcia*, 702 F.3d at 793. The SCA further defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *See* 18 U.S.C. § 2510(17).

Here, the discovery materials establish that the Shareaza LE software obtained information regarding Clements' search term history. *See* Exhibit "F." Clements' specific search terms constitute electronic communications or transmissions that are otherwise protected from third-party disclosure. As aforementioned, a user's search term history would not be accessible to other users of the P2P network using the publicly available version of Shareaza. Thus, to the extent that law enforcement obtained Clements' search term history from Shareaza through operation of the Shareaza LE software, its conduct clearly violated the SCA.

Again, the undersigned acknowledges that there is no per se statutory requirement for the suppression of evidence seized in violation of the SCA. However, for the reasons heretofore explained, counsel submits that the SCA violation is relevant to the Court's disposition of this matter. Furthermore, Clements' maintains that suppression of the

evidence is warranted under Fourth Amendment jurisprudence.

D. The Shareaza LE software's continuous monitoring of Clements' activity violated his Fourth Amendment rights.

Law enforcement routinely utilizes technology in order to conduct investigations of alleged criminal activity. Courts must be concerned with establishing limitations upon the power of technology to ensure that citizens' guaranteed privacy is not eviscerated. Recently, the United States Supreme Court considered whether law enforcement's warrantless utilization of a GPS tracking device on a vehicle violated the defendant's Fourth Amendment right against unreasonable searches and seizures. *See United States v. Jones*, 2012 WL 171117 (Jan. 23, 2012).

The underlying case, *United States v. Maynard*, 615 F.3d 544, 559 (D.C. Cir. 2010), involved two nightclub owners in the District of Columbia, one of whom was Defendant Jones, who were under investigation for narcotics violations. *Id.* at 549. During the investigation, officers attached a GPS device to Jones's vehicle without a warrant. *Id*. at 558–59. The GPS device tracked Jones's movements twenty-four hours a day for one month. *Id*. *Maynard* found that the use of GPS to track the defendant's movements around the clock for an entire month, without a warrant, violated the Fourth Amendment. *Id*. at 559. The Court of Appeals explained that "[p]rolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation."

The United States Supreme Court found that the installation of a GPS monitoring device constituted a warrantless search subject to suppression under the Fourth Amendment. *Jones*, 2012 WL 171117. Justice Scalia's Majority Opinion noted that it "is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id.* at *3. While the Government's physical intrusion was a cornerstone of the Majority's reasoning, the Court did not imply that its decision would have been different had there not been an initial trespass: "our cases suggest that such visual observation is constitutionally permissible. It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question." *Jones*, 2012 WL at *7.

Although the Supreme Court declined to consider whether the installation of GPS is a search that *requires* a warrant, at least four (4) members of the Court suggested that long-term monitoring of a GPS device would necessitate a warrant. Justice Alito's concurrence (joined by Justices Ginsburg, Breyer and Kagan), argued that the Court should apply a more *Katz*-oriented analysis in considering whether GPS monitoring intrudes on an expectation of privacy that society recognizes as reasonable: "[u]nder this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable." *Id*. at *17. Justice Alito also opined that courts should consider the nature of the offense being investigated in

determining the reasonableness of the Government's conduct:

> [b]ut the use of longer-term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. *Id*.

The United States Supreme Court has consistently maintained that "the primary reason for the warrant requirement is to interpose a neutral and detached magistrate between the citizen and the officer engaged in the often competitive enterprise of ferreting out crime." *United States v. Karo*, 468 U.S. 705, 717 (1984); *Johnson v. United States*, 333 U.S. 10 (1948). Respectfully, the same principles and rationale underlying the *Jones* decision are equally applicable to the case at bar. Here, law enforcement used the Shareaza LE software to continuously monitor Clements' computer while it was connected to the P2P network. This monitoring allowed the Government to view his searches through the P2P network without limitation and in the absence of any warrant. Through use of the Shareaza LE software, the Government unilaterally decided who the software would monitor and the length of time that such monitoring would occur. These decisions were made without Clements' knowledge or consent and without prior judicial consideration and/or authorization.

Furthermore, the mere fact that the Shareaza LE software may provide information that could have been obtained through ordinary surveillance does not affect its legality. The Shareaza LE software permits surveillance far beyond the ordinary powers of observation, a point which is inferentially conceded by the Government's use of that

software in their investigations of child pornography cases. In this regard, the Shareaza LE software's value lies in its ability to convey information not otherwise available to the Government.

The undersigned respectfully submits that the warrantless use of the Shareaza LE software in the case at bar implicates the same Fourth Amendment concerns at issue in *Jones*, *supra*. It is axiomatic that Clements' Fourth Amendment rights are superior to the Government's interest in efficient and expedient investigations. As the United States Supreme Court explained over forty years ago, "[w]e downgrade the Fourth Amendment when we forgive noncompliance with its mandate and allow these easier methods of the police to thrive." *Osborn v. United States*, 385 U.S. 323, 329 (1966).

III. CONCLUSION

Counsel respectfully submits that the Government's use of the Shareaza LE software without a warrant violated Clements' Fourth Amendment rights under the United States Constitution. Both Ms. Loehrs' Affidavit and the recorded demonstration confirm that a user's search term history would not be accessible to other P2P network users operating the publicly available version of Shareaza. In this regard, the Shareaza LE software allowed the Government to obtain information that was not publicly available to other users of the P2P network and was thus not in "plain view." Likewise, as discussed in *Jones*, *supra*, the Government's continuous – and seemingly autonomous – monitoring of Clements' computer activity, including his search term history through the P2P network, violates the spirit and purpose of the Fourth Amendment.

Because the Shareaza LE software provided the Government with information that was not in "plain view" or otherwise publicly available, the use of said software constitutes a search and seizure under Fourth Amendment jurisprudence. Furthermore, the Government's failure to secure a warrant prior to using the Shareaza LE software requires suppression of all evidence seized pursuant to the Shareaza LE software. This includes all evidence seized during the course of the undercover investigation (*i.e.* "direct" evidence") as well as any evidence seized through reliance on such information (*i.e.* the fruit of the poisonous tree).

In addition to constituting a violation of the Fourth Amendment, the Government's use of the Shareaza LE software also violated the federal Wiretap Act and the SCA. Specifically, the Shareaza LE software allowed the Government to intercept, access, or otherwise obtain Clements' private electronic communications (*i.e.* search terms) despite the fact that the Government was not a party to said communications.

Clements' has also established that Shareaza LE software conducted a warrantless search of his computer for files that were not publicly available or in "plain view." As set forth in Ms. Loehrs' Affidavit, there is no evidence that the particular files that the Shareaza LE software identified and downloaded were ever in the shared folder of his computer. Because only materials contained in the shared folder of a computer can be considered publicly available or in plain view, the Shareaza LE software conducted a warrantless search of Clements' computer mandating the suppression of evidence.

At the very least, counsel submits that Clements has made a sufficient showing regarding the relevance and necessity of subjecting the Shareaza LE software to

independent forensic testing in this case. Despite the Government's contentions, it is clear that the Shareaza LE software does not operate in the limited capacity as maintained by the Government. Rather, the Shareaza LE software provides law enforcement with private citizens' search term history as well as access to portions of the users' computers that have not been made publicly available.

Irrespective of these issues, Clements is not obligated to merely rely upon the Government's representations concerning the reliability and/or functionality of the software or that his own separate investigation would be unfruitful. *United States v. Budziak*, 697 F.3d 1105, 1113 (9th Cir. 2012). This is especially true when considering the following undisputed facts: the Government did not develop the Shareaza LE software and does not have access to the source code; without the source code, the Government cannot definitively state how the software operates, including whether it allows the Government to access information that is not in "plain view" or otherwise publicly available; and that the Shareaza LE software has never been independently tested or subjected to any peer review.

As to the latter point, it is interesting to note that the Shareaza LE software has never been independently tested or disclosed despite directives from numerous courts in other jurisdictions throughout the United States. *See*, *e.g.*, *United States v. Todd Hartman*, 8:15-cr-00063 (U.S. D.C. CA 2015) (doc. 87)[6]; *United States v. John Crowe*, 1:11-cr-01690 (U.S. D.C.

[6] The Order is attached hereto as Exhibit "H" and is incorporated herein by express reference.

N.M. 2013) (doc. 88)[7]; *United States v. Angel Ocasio*, 3:11-cr-02728 (U.S. D.C. W.D. TX 2013) (doc. 150).[8] The refusal to provide access to the Shareaza software is particularly concerning when considering that all of the questions and arguments set forth herein can be adequately resolved through independent testing.

The only justifications offered by the Government in opposition to this request are that the software is sensitive, proprietary and non-public. Counsel respectfully submits that this Honorable Court is capable of fashioning an Order that adequately protects these interests – e.g. through the issuance of strict protection Orders prohibiting the disclosure or dissemination of any information obtained during the course of the independent evaluation of the Shareaza LE software – while simultaneously recognizing Clements' important constitutional rights, including his right to due process of law, the right to prepare an effective defense and the right to confrontation.

[7] The Order is attached hereto as Exhibit "I" and is incorporated herein by express reference.

[8] The Order is attached hereto as Exhibit "J" and is incorporated herein by express reference.

WHEREFORE, Defendant, John Clements, hereby respectfully requests that this Honorable Court issue an Order suppressing any and all evidence obtained by the Government – both directly and indirectly – through the use of the Shareaza LE software in the case at bar. Such request includes any evidence produced during the undercover investigation of this case as well as all evidence seized pursuant to the search warrant that was executed on June 3, 2014. Alternatively, counsel requests that the Court reconsider its previous denial of Defendant's Motion to Compel, and Order the Government to allow independent forensic testing of the Shareaza LE software forthwith.

Respectfully submitted,

/s/ Eric C. Nemecek
IAN N. FRIEDMAN (0068630)
ERIC C. NEMECEK (0083195)
Counsel for Defendant
Friedman & Nemecek, L.L.C.
1360 E. 9th Street, Suite 650
Cleveland, OH 44114
Phone: (216) 928-7700
Email: inf@fanlegal.com
ecn@fanlegal.com